APPENDIX A

CLAIMS

1. (previously presented) A method for verifying an identity of a new-user of a computer system, comprising:

   a. receiving at least one identity attribute from the new-user;
   b. similarity searching the at least one new-user identity attribute against at least one database of denied-user identity attributes;
   c. receiving a similarity search result;
   d. determining a positive or negative similarity match between the at least one new-user identity attribute and the denied-user identity attributes based on the similarity search results;
   e. allowing the new-user to access the computer system, where a negative similarity match has been determined; and
   f. denying the new-user access to the computer system, where a positive similarity match has been determined.

2. (original) The method of claim 1, wherein the at least one new-user identity attribute comprises a new-user profile.

3. (original) The method of claim 2, wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles.

4. (original) The method of claim 3, wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database.

5. (previously presented) The method of claim 1, wherein the step of determining a positive or negative similarity match further comprises comparing the similarity search result to a first match tolerance level.

6. (previously presented) The method of claim 5, wherein a positive similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level.

7. (previously presented) The method of claim 5, wherein a negative similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match tolerance level.

8. (previously presented) The method of claim 1, further comprising, where a positive similarity match has been determined, verifying the positive similarity match via a secondary review, after the step of determining whether a positive or negative similarity match exists and before the step of denying the new-user access to the computer system.

9. (previously presented) The method of claim 8, wherein the step of verifying the positive similarity match further comprises comparing the similarity search result to a second match tolerance level.

10. (previously presented) The method of claim 8, further comprising allowing the new-user to access the computer system, where the positive similarity match does not meet or exceed the second match tolerance level.

11. (previously presented) The method of claim 8, further comprising denying the new-user access to the computer system, where the positive similarity match meets or exceeds the second match tolerance level.

12. (previously presented) The method of claim 1, further comprising, after determining whether a positive or negative similarity match exists, the steps of:

adding the new-user identity to at least one database of valid user identities, where a negative similarity match has been determined; and adding the new-user identity attributes to the at least one database of denied-user identity attributes, where a positive similarity match has been determined.

13. (original) The method of claim 1, wherein the at least one new-user identity attribute is received from at least one component, chosen from a group consisting of Internet web sites, relational databases, data entry systems, and hierarchical databases.

14. (original) The method of claim 1, wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes.

15. (canceled)

16. (previously presented) A method for verifying an identity of a new-user of a computer system, comprising:

a. receiving at least one identity attribute from the new-user;

b. similarity searching the at least one identity attribute against at least one database of denied-user identity attributes;

c. receiving a similarity search result;

d. determining a positive or negative similarity match between the at least one new-user identity attribute and the denied-user identity attributes based on the similarity search result;

e. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where a negative similarity match has been determined;

f. where a positive similarity match has been determined, verifying the positive similarity match via a secondary review;

g. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where the positive similarity match is not verified; and

h. denying the new-user access to the computer system and adding the at least one new-user identity attribute to at least one database of denied-user identity attributes, where the positive similarity match is verified.

17. (original) The method of claim 16, wherein the at least one new-user identity attribute comprises a new-user profile.

18. (original) The method of claim 17, wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles.

19. (original) The method of claim 18, wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database.

20. (previously presented) The method of claim 16, wherein the step of determining a positive or negative similarity match further comprises comparing the similarity search result to a first match tolerance level.

21. (previously presented) The method of claim 20, wherein a positive similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level.

22. (previously presented) The method of claim 20, wherein a negative similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match tolerance level.

23. (previously presented) The method of claim 16, wherein the step of verifying the positive similarity match further comprises comparing the similarity search result to a second match tolerance level.

24. (previously presented) The method of claim 16, wherein the at least one new-user identity attribute is received from at least one component, chosen from a group consisting of Internet web sites, relational databases, data entry systems, and hierarchical databases.

25. (previously presented) The method of claim 16, wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes.

26. (canceled)

27. (previously presented) A system for verifying an identity of a new-user of a computer system, comprising:

a means for receiving at least one identity attribute from the new-user;

at least one database for storing denied-user identity attributes;

at least one database for storing valid user identities;

a means for similarity searching the at least one identity attribute against the at least one database of denied-user attributes;

a means for determining a positive or negative similarity match between the at least one new-user attribute and the at least one database of denied-user identity attributes;

a means for allowing the new-user to access the computer system, where a negative similarity match has been determined;

a means for denying the new-user access to the computer system, where a positive similarity match has been determined;

a means for adding the new-user identity to the at least one database for storing valid user identities, where a negative similarity match has been determined; and

a means for adding the at least one new-user identity attribute to the at least one database of denied-user attributes, where a positive similarity match has been determined.

28 (previously presented) A computer-readable medium containing instructions for controlling a computer system to implement the method of claim 1.

29 (previously presented) A computer-readable medium containing instructions for controlling a computer system to implement the method of claim 16.

30. (previously presented) A method for verifying an identity of a new user of a computer system, comprising:

similarity searching one or more new user identity attribute profile data records against denied-user identity attribute profile data records;

receiving one or more similarity search results sets, each result set having a corresponding new user identity attribute profile data record and a corresponding similarity match score;

comparing each similarity match score with a pre-determined match tolerance level for determining negative similarity match scores and positive similarity match scores;

for each negative similarity match score having a value of less than or equal to the pre-determined match tolerance level, allowing access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a negative similarity match score; and

for each positive similarity match score having a value greater than the pre-determined match tolerance level, denying access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score.

31. (previously presented) The method of claim 30, wherein the step of denying access comprises:

confirming whether the positive similarity match score exists between the new user identity attribute profile data record and a corresponding suspended-users identity attribute profile data record;

allowing a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score to access the computer system, where the positive similarity match score is not confirmed; and

denying a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score access to the computer system, where the positive similarity match score is confirmed.